

UNITED STATES DISTRICT COURT

for the
Southern District of OhioIn the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*Motorola Cell Phone, IMEI: 359115100497646;
Samsung Galaxy S10e, IMEI: 354764100128555;
Apple iPhone in black protective case.

Case No. 3:20Mj151

APPLICATION FOR A SEARCH WARRANT BY TELEPHONE OR OTHER RELIABLE
ELECTRONIC MEANSI, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
SEE ATTACHMENT Alocated in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
21 USC 846 and 841(a)(1) &
(b)(1)(A)Offense Description
Conspiracy to possess with intent to distribute 400 grams or more of fentanyl, a
scheduled II controlled substance

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested
 under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA ANDREW MALADY, HSI

Printed name and title

Sworn to before me and signed in my presence via facetime.

Date: 03/19/2020

Judge's signature

City and state: Dayton, Ohio

Sharon L. Ovington, U. S. Magistrate Court

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF:

Motorola Cell Phone, IMEI:
359115100497646;
Samsung Galaxy S10e, IMEI:
354764100128555;
Apple iPhone in black protective case.

3:20mj151

Case No. _____

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Andrew Malady, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I, Andrew Malady, am a Special Agent of Homeland Security Investigations (HSI), United States Department of Homeland Security. As such, I set forth the following in support of a search warrant authorizing the examination of: one (1) Motorola Cell Phone, IMEI: 359115100497646 (Subject Device 1); one (1) Samsung Galaxy S10e, IMEI: 354764100128555 (Subject Device 2); one (1) Apple iPhone in black protective case (Subject Device 3), and the extraction from Subject Devices 1 through 3 of electronically stored information described in Attachment B. Subject Devices 1 through 3 are currently within the Southern District of Ohio in the custody of HSI.

2. I am an employee of Homeland Security Investigations assigned to the Cincinnati Resident Office. I have been employed with HSI since May of 2015. I attended and graduated from the basic agent training course in Brunswick, Georgia. Prior to this, I was a Border Patrol

Agent for over seven years with the United States Border Patrol in Douglas, Arizona. I have received extensive training in the investigation of narcotics trafficking and financial crimes from the United States Border Patrol and Homeland Security Investigations, as well as ongoing in-service training.

3. Between February 2018 and August 2018, and again since September 2019, I have been assigned to the Homeland Security Investigations (HSI) Border Enforcement Security Task Force (BEST) in Dayton, Ohio.

4. As a Special Agent for HSI, I am charged with the duty of enforcing among other Titles, the Controlled Substance Act, Title 21, United States Code, together with other assigned duties as imposed by federal law.

5. By virtue of my employment with HSI, I perform and have performed various tasks which include, but are not limited to:

- a. Functioning as a surveillance agent for the primary purpose of observing and movements of drug traffickers and those suspected of trafficking in drugs;
- b. Functioning as a case agent which entails the supervision of specific aspects of drug investigations; and,
- c. Tracing and tracking monies and assets gained by drug traffickers from the illegal sale of drugs.

6. This Affidavit seeks the issuance of a search warrant. There is probable cause Jaime Josue ORDAZ, violated Title 21 U.S.C. § 846 and 841 (b)(1)(A) (conspiracy to possess with intent to distribute 400 grams or more of fentanyl). All of the details of the investigation are not included in this Affidavit, rather only information necessary to establish probable cause to search Subject Devices 1 through 3. There is probable cause to believe that evidence of these

violations is contained within the cellular telephones as further described and depicted in Attachment A. The information contained in this affidavit comes from my personal knowledge and facts relayed to me by other law enforcement officers.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

7. The property to be searched is a
 - a. one (1) Motorola Cell Phone, IMEI: 359115100497646 (Subject Device 1);
 - b. one (1) Samsung Galaxy S10e, IMEI: 354764100128555 (Subject Device 2);
 - c. one (1) Apple iPhone in black protective case (Subject Device 3).

Subject Devices 1 through 3 are currently located at HSI at the HSI Evidence Room, located at 9875 Redhill Dr., Blue Ash, OH 45242 (and within the Southern District of Ohio). Subject Devices 1 through 3 are depicted and described in Attachment A.

8. The applied-for warrant would authorize the forensic examination of Subject Devices 1 through 3 for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

9. Together with agents and officers of the HSI Cincinnati Border Enforcement Security Task Force ("BEST"), I am currently involved in the investigation related to the drug offenses believed to have been committed by Jaime Josue ORDAZ (ORDAZ). Based upon the investigation to date, there is probable cause to believe that ORDAZ violated Title 21 U.S.C. §§ 846 and 841 (b)(1)(A) (conspiracy to possess with intent to distribute 400 grams or more of

fentanyl). Unless otherwise noted, when I assert that a statement was made, I received the information from a law enforcement officer who provided the information to me, either verbally or in a written report. The officer providing me with the information may have received the information by way of personal knowledge or from another source.

10. On March 9, 2020, the Ohio State Highway Patrol (OSP) was conducting patrol at or near Interstate 70 near State Route 235 when they observed a Semi-truck, with California license plate XP50411 hauling a trailer bearing Maine license plate 2454258, exiting Interstate 70 onto State Route 235.

11. At approximately 9:10pm, OSP observed a traffic violation and conducted a traffic stop on the Semi-truck. During the traffic stop, the driver was identified as Jaime Josue **ORDAZ**, who produced a State of California driver's license. A criminal history check showed **ORDAZ** had prior arrests for bulk cash smuggling and transporting narcotics.

12. During the traffic stop, an OSP trooper deployed his drug detection canine partner, who conducted a free air sniff of the vehicle. After receiving a positive alert on the vehicle, a probable cause search was conducted. During the search of the cab, OSP located a bag containing twelve (12) brick-shaped packages that later tested positive for fentanyl. During a search of the trailer, OSP located an additional four (4) brick-shaped packages in a box that later field tested positive for cocaine.

13. **ORDAZ** was advised of his constitutional rights per Miranda. **ORDAZ** stated he understood his rights. **ORDAZ** did not have anything to say regarding what was found in the vehicle and did not want to answer any questions from Agents.

14. Subject Devices 1 through 3 are in the lawful possession of HSI. During the encounter with **ORDAZ**, Subject Devices 1 and 2 were located in the cab of the Semi-truck

ORDAZ was driving. Subject Device 3 was located on **ORDAZ**'s person during a pat-down. Subject Devices 1 through 3 were seized as evidence.

15. I believe Subject Devices 1 through 3 may contain evidence of communication between **ORDAZ** and additional known and unknown co-conspirators and other evidence related to drug trafficking. I request permission to search the electronic data stored in Subject Devices 1 through 3 to locate any other evidence of drug trafficking activity that may be inside.

16. In my experience, cellular phones are often used by criminals to carry out their business. Criminals often use the phones to communicate (either by voice, text message, or internet-based communication accessed by the phone) with customers, suppliers, and associates about pending criminal activity. It is also common to find photographs of their criminal associates stored on the phones, as well as photos of weapons, drugs, money, or assets associated with their illegal activity. Criminals will often store phone numbers for their associates in the cellular phone, and sometimes use alias or code names for those entries. Electronic evidence stored on the phone also can show who used a particular cellular phone, because criminals often use prepaid phones or fake subscriber names when obtaining the phone from the service provider. Criminals commonly have multiple phones at a given time, with certain phones used to communicate with particular individuals or for specific purposes. By searching the data stored on the phones, I believe evidence of **ORDAZ**'s criminal activity may be revealed.

17. Subject Devices 1 through 3 are currently in the lawful possession of HSI. Subject Devices 1 through 3 came into HSI's possession after the Devices were seized during the course of the aforementioned traffic stop.

18. Based on my training and experience, I know that Subject Devices 1 through 3 have been stored in a manner in which the contents are, to the extent material to this

investigation, in substantially the same state as they were when the Subject Devices first came into the possession of HSI.

TECHNICAL TERMS

19. Based upon my training and experience, I use the following technical terms to convey the following meanings:

- a. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. **Digital camera:** A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. **GPS:** A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved

in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. **IP Address:** An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

20. Based on my training, experience, and research, I know that Subject Devices 1 through 3 are cellular telephones, and that most modern cellular telephones have capabilities that allow them to serve as “a wireless telephone, digital camera, portable media player, GPS navigation device, and PDAs.” In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Subject Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on these Subject Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

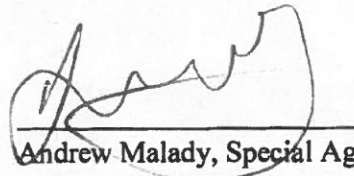
23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of Subject Devices 1 through 3 consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to, computer-assisted scans of the entire medium that might expose many parts of Subject Devices 1 through 3 to human inspection in order to determine whether it is evidence described by the warrant.

24. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

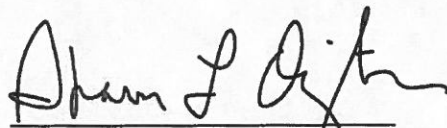
CONCLUSION

25. For these reasons, I submit that this affidavit supports probable cause for a search warrant authorizing the examination of Subject Devices 1 through 3 described in Attachment A, to seek the items described in Attachment B, which are evidence of violation of Title 21 U.S.C. §§ 846 and 841 (b)(1)(A) (conspiracy to possess with intent to distribute 400 grams or more of fentanyl).

Respectfully submitted,


Andrew Malady, Special Agent
Homeland Security Investigations

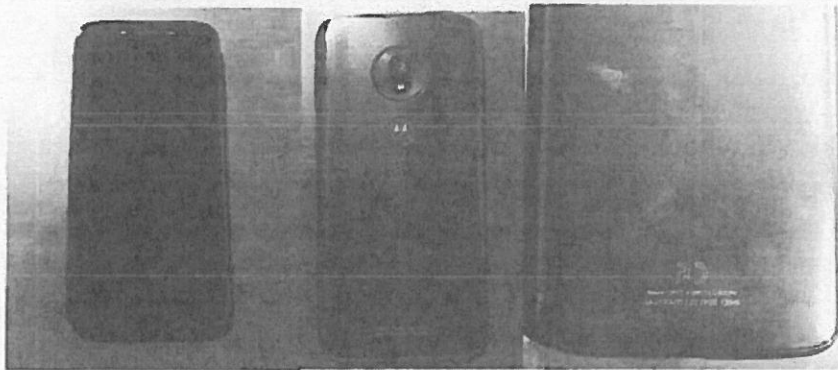
Subscribed and sworn to before me on March 19, 2020.


Honorable Sharon L. Ovington
United States Magistrate Judge

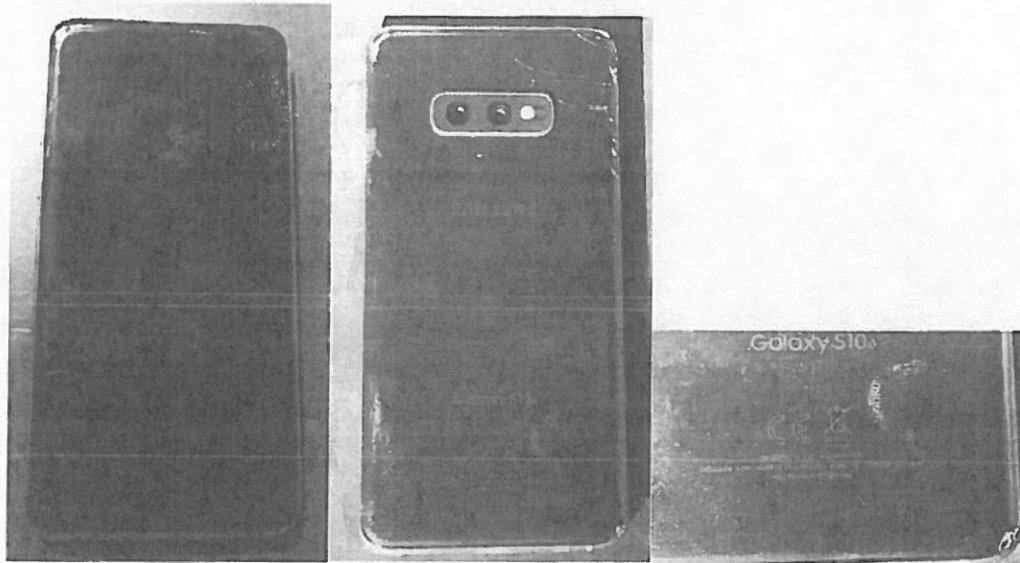
ATTACHMENT A

This warrant applies to the following devices:

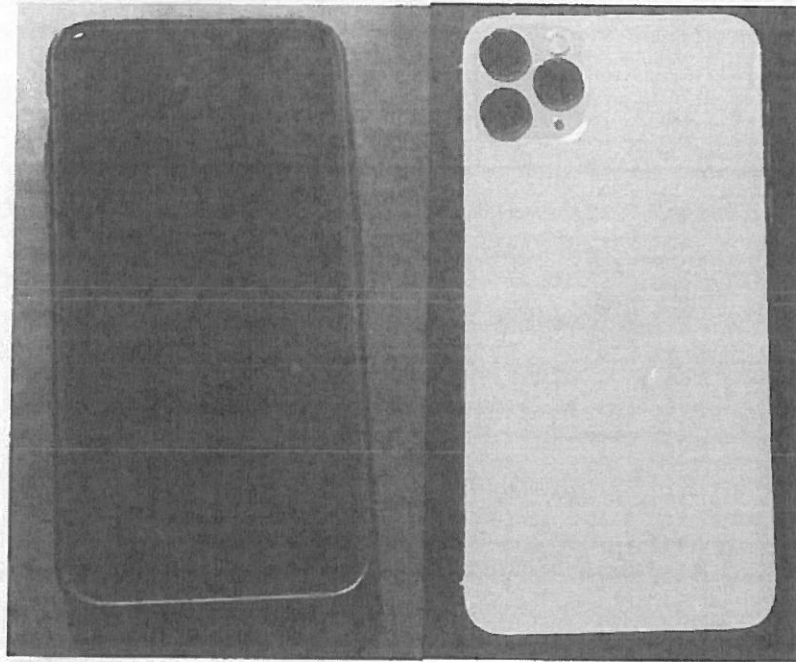
1. One (1) Motorola Cell Phone, IMEI: 359115100497646, together with all electronic devices, including Subscriber Identity Modules, or SIM cards, contained therein (Subject Device 1). Subject Device 1 is currently located in the custody of HSI at the HSI Evidence Room, located at 9875 Redhill Dr., Blue Ash, OH 45242 (and within the Southern District of Ohio). It is depicted in the photographs below:



2. One (1) Samsung Galaxy S10e, IMEI: 354764100128555, together with all electronic devices, including Subscriber Identity Modules, or SIM cards, contained therein (Subject Device 2). Subject Device 2 is currently located in the custody of HSI at the HSI Evidence Room, located at 9875 Redhill Dr., Blue Ash, OH 45242 (and within the Southern District of Ohio). It is depicted in the photographs below:



3. One (1) Apple iPhone in black protective case, together with all electronic devices, including Subscriber Identity Modules, or SIM cards, contained therein (Subject Device 3). Subject Device 3 is currently located in the custody of HSI at the HSI Evidence Room, located at 9875 Redhill Dr., Blue Ash, OH 45242 (and within the Southern District of Ohio). It is depicted in the photographs below:



This warrant authorizes the forensic examination of Subject Device 1, Subject Device 2, and Subject Device 3 for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on Subject Devices 1 through 3 described in Attachment A that relate to violations of Title 21 U.S.C. § 846 and 841 (b)(1)(A), involving Jaime Josue ORDAZ, including but not limited to:

- a. Lists of contacts and related identifying information;
- b. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- c. Any information related to transferring, transporting of currency to include banking information;
- d. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
- e. Any information recording ORDAZ's schedule or travel, such as the use of hotel rooms or other lodging, rental cars, or airline information; all bank records, checks, credit card bills, account information, and other financial records.
- f. Evidence of communication and association between ORDAZ's co-conspirators, including "WhatsApp" or other cell phone applications used to communicate, text messages, photographs, email, Facebook, or other social media, phone call logs, and stored phone numbers;
- g. Evidence of user attribution showing who used or owned the Subject Devices at the time the items described in this warrant were created, edited, or deleted, such

as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

- h. Records evidencing the use of any Internet Protocol addresses to communicate with Facebook or any other website, including:
 - i. Records of Internet Protocol addresses used;
 - j. Records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.